

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-259569  
 (43)Date of publication of application : 22.09.2000

(51)Int.Cl. G06F 15/00  
 G06F 12/14  
 G06F 13/00

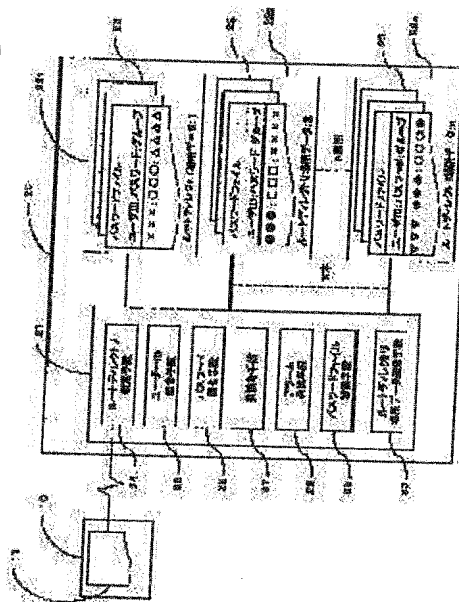
(21)Application number : 11-066666 (71)Applicant : NEC ENG LTD  
 (22)Date of filing : 12.03.1999 (72)Inventor : SHINKAWA YOSHIHIKO

## (54) METHOD AND SYSTEM FOR CERTIFYING PASSWORD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To block the illegal invasion of the third person to an information communication network system even when a password is stolen by the third person in the information network communication system.

**SOLUTION:** Inside a server 20, route directories 221-22n are prepared at plural spots for storing a password file 23 for each user. At the time of access, a user ID, a password and the place data of the route directory storing the password file 23 are transmitted to the server 20 and when a password recorded in the password file 23 of the relevant route directory is coincident with a password sent from an access terminal, log-in to the server 20 is permitted. At the same time, at the time of log-out, the place of the route directory storing the password file 23 is moved from the route directory at random and the place data of that moved route directory are stored in a storage part 11 of an access terminal 10.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-259569  
(P2000-259569A)

(43) 公開日 平成12年9月22日 (2000.9.22)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ターミナル* (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 C 5 B 0 8 5
13/00	3 5 1	13/00	3 5 1 Z 5 B 0 8 9

審査請求 未請求 請求項の数2 O L (全 8 頁)

(21) 出願番号 特願平11-66666

(22) 出願日 平成11年3月12日 (1999.3.12)

(71) 出願人 000232047

日本電気エンジニアリング株式会社  
東京都港区芝浦三丁目18番21号

(72) 発明者 新川 仁彦

東京都港区芝浦三丁目18番21号 日本電気  
エンジニアリング株式会社内

(74) 代理人 100106563

弁理士 中井 潤

Fターム(参考) 5B017 AA01 AA04 BA05 BA07 BA10

BB02 BB07 BB09 CA16

5B085 AE03 AE08 BG07

5B089 GA11 GA21 JB22 KA17 KB13

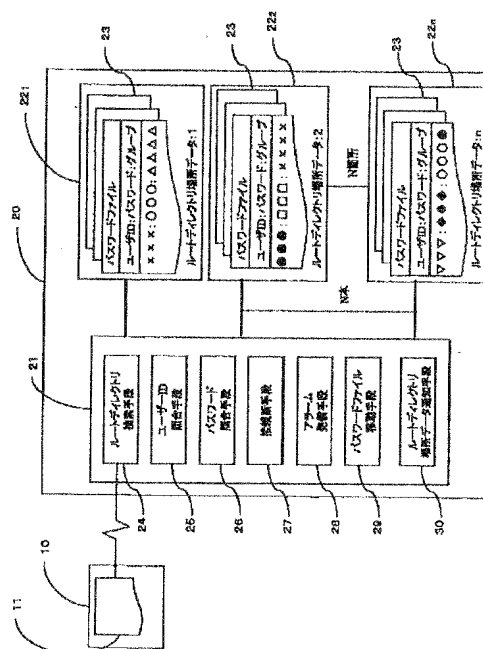
KC44 KC58 KG10

(54) 【発明の名称】 パスワード認証方法及びパスワード認証システム

(57) 【要約】

【課題】 情報ネットワーク通信システムにおいて、パスワードを第三者に盗まれても、第三者による情報通信ネットワークシステムへの不正侵入を阻止する。

【解決手段】 サーバー20内に、ユーザー毎のパスワードファイル23を格納するための複数箇所のルートディレクトリ22<sub>1</sub>~22<sub>n</sub>を用意し、アクセス時にユーザーID、パスワード及びパスワードファイル23を格納したルートディレクトリの場所データとをサーバー20に送信し、該当するルートディレクトリのパスワードファイル23に記録されたパスワードが一致したときにサーバー20へのログインを許可するとともに、ログアウト時にはパスワードファイル23を格納したルートディレクトリをそれまで格納していたルートディレクトリからそれ以外のルートディレクトリにランダムに場所移動し、該場所移動したルートディレクトリの場所データをアクセス端末10の記憶部11に記憶する。



## 【特許請求の範囲】

【請求項 1】 サーバーと、該サーバーに通信回線を介して接続される複数のアクセス端末とで構成される情報通信ネットワークシステムにおいて、前記サーバー内に、ユーザー ID とパスワードを記録するためのパスワードファイルを各ユーザー毎に用意するとともに、これらパスワードファイルを格納するための複数箇所のルートディレクトリを用意し、

サーバーへのアクセス時に、アクセス端末から自己のユーザー ID と、パスワードと、これらユーザー ID とパスワードを記録したパスワードファイルを格納したルートディレクトリの場所データとをサーバーに送信し、該当するルートディレクトリのパスワードファイルに記録されたパスワードがアクセス端末から送られてきたパスワードと一致したときにサーバーへのログインを許可するとともに、

ログアウト時にはパスワードファイルをそれまで格納していたルートディレクトリからそれ以外のルートディレクトリにランダムに場所移動し、該変更したルートディレクトリの場所データを対応するアクセス端末に送信してアクセス端末内に記憶することを特徴とするパスワード認証方法。

【請求項 2】 サーバーと、該サーバーに通信回線を介して接続される複数のアクセス端末とで構成される情報通信ネットワークシステムにおいて、前記各アクセス端末に、前記サーバーから送られてくる自己のパスワードファイルについてのルートディレクトリの場所データを格納記憶する記憶部を備えるとともに、前記サーバー内には、

各ユーザー毎に用意したユーザー ID とパスワードを記録するためのパスワードファイルを格納する複数箇所のルートディレクトリと、

アクセス端末から送信されるルートディレクトリの場所データに対応したルートディレクトリを検索するルートディレクトリ検索手段と、

アクセス端末から送信されたユーザー ID に対応するパスワードファイルが前記ルートディレクトリ検索手段によって検索されたルートディレクトリ内に存在するか否かを照合するユーザー ID 照合手段と、

アクセス端末から送信されたパスワードが前記ユーザー ID 照合手段で選択されたパスワードファイルに記録されたパスワードと一致するか否かを照合するパスワード照合手段と、

少なくともアクセス端末から前記ルートディレクトリの場所データが送信されてこない場合には通信回線を自動的に切断する接続断手段と、

アクセス端末からサーバーにログインした正規ユーザーのログアウト時に、パスワードファイルをそれまで格納していたルートディレクトリからそれ以外の他のルート

ディレクトリにランダムに場所移動するパスワードファイル移動手段と、

該パスワードファイル移動手段によって変更されたルートディレクトリの場所データを対応するアクセス端末に向けて送信するルートディレクトリ場所データ通知手段とを備えたことを特徴とするパスワード認証システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、サーバーと、該サーバーに通信回線を介して接続される複数のアクセス端末とで構成される情報通信ネットワークシステムにおいて、サーバーへの不正侵入を阻止し、セキュリティの強化を図るためのパスワード認証方法とパスワード認証システムに関する。

## 【0002】

【従来の技術】 セキュリティを考慮した情報通信ネットワークシステムにログインする場合には、正規のユーザーであるかどうかを認証するために、情報通信ネットワークシステムのサーバーはアクセス端末に対してパスワードの入力を要求する。そして、ログインしようとするユーザーは、予めサーバーに登録しておいた文字列となるパスワードをアクセス端末のキーボードから入力する。情報通信ネットワークシステムのサーバーは、この入力された文字列と予め登録されている文字列とが一致するか否かをユーザー ID とパスワードを記録したパスワードファイルにアクセスして判定し、一致すれば本人であると認証してログインを許可する。

【0003】 サーバー内では、パスワードファイルは符号化・暗号化されて格納されているが、セキュリティの上では、各ユーザーが採用する生のパスワード自体も第三者に容易に推測されないものであることが望ましい。しかしながら、一般に全く意味のない文字や数字はパスワードとして覚えるのが大変であるため、多くのユーザーは辞書に載っている単語や自分の生年月日あるいは電話番号等、身近で第三者が簡単に推測できる単純な文字列をパスワードにしてしまうことが多い。また、たとえ簡単に推測できないようなパスワードを採用したとしても、第三者の前でキーボードからパスワードを入力するような場合には、入力する手の動きから第三者にパスワードを知られることがある。

【0004】 さらに、パスワードファイルは符号化・暗号化されているものの、通常、全てのユーザーのパスワードファイルを 1 ヶ所のルートディレクトリにまとめて格納しているため、正規ユーザーでない第三者が何らかの方法で通信ネットワークシステムに不正侵入した場合、全てのユーザーについての全てのパスワードを盗むことが可能となり、リモートで情報通信ネットワークシステムに対して不正な侵入を容易に許してしまうおそれがある。

## 【0005】

証システムの実施の形態の具体例を図面を参照しながら説明する。

【0013】図1は、本発明にかかるパスワード認証システムの第1実施例を示すブロック図である。ネットワークのアクセス端末10は、ルートディレクトリ場所データを格納するための記憶部11を備え、情報通信ネットワークシステムの中核をなすサーバー20は、中央処理制御部21と、複数（ $n$ 箇所）のルートディレクトリと、各ルートディレクトリ22<sub>1</sub>～22<sub>n</sub>に分散格納されたユーザー単位ごとのパスワードファイル23を備え

る。

【0014】前記中央処理制御部21は、ルートディレクトリ検索手段24と、ユーザーID照合手段25と、パスワード照合手段26と、接続断手段27と、アラーム発信手段28と、パスワードファイル移動手段29と、ルートディレクトリ場所データ通知手段30とで構成されている。尚、中央処理制御部21は、CPUやメモリ等によって構成されており、各手段24～30は中央処理制御部21内に格納された制御処理プログラムによってソフトウェア的に実現されている。

【0015】図2は、前記パスワード認証システムにおけるパスワードの認証動作の処理手順を示すフローチャートである。この図2を参照して、図1のパスワード認証システムのパスワード認証動作について説明する。

【0016】本発明のパスワード認証システムは、予め、初期設定として各ユーザー毎にパスワードファイル23を作成し、このユーザー毎のパスワードファイル23に各々のユーザーIDとパスワードを記録した上で、各々のパスワードファイル23をサーバー20内の $n$ 箇所のルートディレクトリ22<sub>1</sub>～22<sub>n</sub>に分散格納するとともに、各アクセス端末10の記憶部11に、自己のパスワードファイル23を格納したルートディレクトリ22<sub>1</sub>～22<sub>n</sub>の場所データを格納記録しておく。

【0017】正規ユーザーが自己のアクセス端末10を通じて情報通信ネットワークシステムのサーバー20にログインする場合には、アクセス端末10のキーボードよりユーザーIDを入力し、サーバー20に送信する（図2のステップS31）。アクセス端末10は、このユーザーIDの送信に併せて、予め記憶部11に格納しておいたルートディレクトリの場所データもサーバー20の中央処理制御部21に送信する（図2のステップS32）。

【0018】サーバー20内の中央処理制御部21は、ルートディレクトリ検索手段24とユーザーID照合手段25とによって、前記送信されてきたルートディレクトリの場所データからルートディレクトリ22<sub>1</sub>～22<sub>n</sub>内の該当するルートディレクトリを選択し、該ルートディレクトリ内にユーザーIDに対応するパスワードファイルが存在するかどうかを検索する（図2のステップS33）。そして、対応するユーザーIDに対応するパス

ワードファイルが存在する場合には、アクセス端末10に対してパスワードの入力を促す。

【0019】正規ユーザーはアクセス端末10のキーボードよりパスワードを入力し、サーバー20の中央処理制御部21に送信する（図2のステップS34）。中央処理制御部21のパスワード照合手段26は、前記検索されたルートディレクトリのパスワードファイル23に格納されているパスワードと、前記送信されてきたパスワードとの照合を行ない（図2のステップS35）、一致していれば正規ユーザーに対してサーバー20へのログインを許可する（図2のステップS36）。これによって、ログインした正規ユーザーは所望の処理を実行する。

【0020】そして、サーバー20にログインした前記正規ユーザーが所望の処理を終了し、サーバー20からログアウトする際には（図2のステップS41）、中央処理制御部21のパスワードファイル移動手段29は、前記正規ユーザーのユーザーIDとパスワードを格納したパスワードファイル23を $n$ 箇所あるルートディレクトリ22<sub>1</sub>～22<sub>n</sub>のうち、それまで格納していたルートディレクトリからそれ以外の他のルートディレクトリに乱数等を利用してランダムに移動させる（図2のステップS42）。

【0021】パスワードファイル23を移動したルートディレクトリの場所データは、中央処理制御部21のルートディレクトリ場所データ通知手段30を通じて対応するアクセス端末10の記憶部11に送信され（図2のステップS43）、アクセス端末10内の記憶部11に記憶されているルートディレクトリの場所データを新しい場所データに書き換える（図2のステップS44）。

【0022】正規ユーザーが再度ログインする際には、前回のログアウト時に記憶部11に格納した新しいルートディレクトリの場所データに基づき、上記したと同様にパスワードの認証を行う（図2のステップS31）。従って、正常なアクセスを行なっている限り、正規ユーザーは何らの規制を受けることなくその都度サーバー20へログインすることができる。

【0023】次に、正規ユーザーでない第三者がパスワードを何らかの方法で盗み出し、該パスワードを用いてリモートから情報通信ネットワークシステムのサーバー20への不正侵入を試みた場合のパスワード認証動作について説明する。

【0024】情報通信ネットワークシステムのサーバー20へ侵入する際、正規ユーザーでない第三者が盗み出したユーザーIDを入力すると（図2のステップS31）、この入力されたユーザーIDは情報通信ネットワークシステムのサーバー20へ送信される（図2のステップS32）。

【0025】しかしながら、入力したユーザーIDとこれに対応したパスワードを記録したパスワードファイル

23が複数箇所のルートディレクトリ22<sub>1</sub>~22<sub>n</sub>中のどのルートディレクトリにあるかというを示す場所データが送信されないため、中央処理制御部21のルートディレクトリ検索手段24とユーザーID照合手段25は、パスワードを検索して一致しているかどうかの判断を行なうことができない(図2のステップS33)。従って、サーバー20は、不正なアクセスであるとして、この正規ユーザーでない第三者のログインを許可しない(図2のステップS37)。

【0026】また、初期設定時のルートディレクトリの場所データを正規ユーザーでない第三者が知っていたとしても、正規ユーザーがサーバー20にログイン・ログアウトする毎に、正規ユーザーのユーザーIDに対応したパスワードファイル23がランダムにルートディレクトリ22<sub>1</sub>~22<sub>n</sub>を移動するので、正規ユーザーでない第三者が現時点におけるユーザーIDに対応したパスワードファイル23のルートディレクトリ22<sub>1</sub>~22<sub>n</sub>の場所データを入手して不正侵入することは不可能である。

【0027】正規ユーザーでない第三者が前記パスワードファイル23をランダムに格納するための全てのルートディレクトリ22<sub>1</sub>~22<sub>n</sub>の場所を知り得た場合には、正規ユーザーでない第三者が情報通信ネットワークシステムのサーバー20へ侵入する確率は、前記ルートディレクトリ22<sub>1</sub>~22<sub>n</sub>の場所数nに対応し、1/nとなる。従って、確率上ではn回の試行により情報通信ネットワークシステムのサーバー20へ不正侵入されることになるが、最初の侵入の際にルートディレクトリ22<sub>1</sub>~22<sub>n</sub>の場所を間違えた時点で、中央処理制御部21の接続断手段27によって当該接続回線を強制的に切断し(図2のステップS37)、アラーム発信手段28から管理者及び正規ユーザーに対してアラームを発信し、不正侵入が発生したことを知らせるとともに、正規ユーザーにパスワードを変更するように促す(図2のステップS38)。これによって、正規ユーザーでない第三者がn回の試行をしても不正侵入することができなくなり、情報通信ネットワークシステムのセキュリティを高めることができる。

【0028】次に、本発明にかかるパスワード認証システムの第2実施例について、図3を参照して説明する。尚、図3中、前記第1実施例(図1)と同一または相当部分には同一の符号を付し、その詳細な説明は省略する。

【0029】この第2実施例にかかるパスワード認証システムは、制御処理プログラムを記録した記録媒体31を外部に、制御処理プログラムを入れ換え自在とした点で前記第1実施例のものと異なるだけである。尚、記録媒体31としては、磁気ディスク、半導体メモリ、その他の記録媒体を利用することができる。

【0030】記録媒体31の制御処理プログラムは、記

録媒体31から中央処理制御部21に読み込まれ、中央処理制御部21は前記第1実施例における中央処理制御部21による処理と同じ処理を実行する。

【0031】すなわち、アクセス端末10より、ユーザーIDとルートディレクトリ場所データが与えられると、中央処理制御部21は、まずルートディレクトリ場所データに基づき、ルートディレクトリ22<sub>1</sub>~22<sub>n</sub>中の指定のルートディレクトリを検索し、ユーザーIDの照合を行う。該照合処理の結果、当該ルートディレクトリにユーザーIDが存在する場合には、パスワードの入力をアクセス端末10に促し、前述した第1実施例と同様にパスワードを照合し、パスワードが一致する場合にはサーバー20へのログインを許可する。

【0032】一方、前記照合処理の結果、該当するルートディレクトリにユーザーIDが存在しない場合には、前記アクセス端末10との接続を断ち、管理者及び正規ユーザーにアラームを発信し、不正侵入が発生したことを知らせるとともに、正規ユーザーにパスワードを変更するように促す。

【0033】サーバー20にログインした正規ユーザーが、サーバー20からログアウトする際には、中央処理制御部21は、前記正規ユーザーのユーザーIDとパスワードを格納したパスワードファイル23をn箇所あるルートディレクトリ22<sub>1</sub>~22<sub>n</sub>のうち、それまで格納していたルートディレクトリからそれ以外の他のルートディレクトリにランダムに移動させ、この移動させたルートディレクトリの場所データをアクセス端末10に送信する。これによって、前記第1実施例と同様に、第三者による不正侵入を阻止することができる。

【0034】

【発明の効果】以上説明したように、本発明のパスワード認証方法とパスワード認証システムによれば、パスワードファイルへのルートディレクトリが複数箇所あるため、パスワードの入力だけではなく、パスワードファイルの存在するルートディレクトリの場所を指定する場所データがなければ、情報通信ネットワークシステムに侵入することができず、さらに、ログアウトごとにランダムにパスワードファイルを格納するルートディレクトリが変わるため、パスワードファイルが格納されているルートディレクトリの場所データを正規ユーザーでない第三者が手に入れることは困難となる。このため、たとえ推測や盗み見等によってパスワードを見破られたとしても、容易にネットワークへ侵入できないようにすることができ、情報通信ネットワークシステムにおけるセキュリティを格段に向上させることができる。

【0035】また、ユーザーごとのパスワードファイルを複数箇所のルートディレクトリに分散して格納することにより、全てのユーザーのパスワードを知るためには複数箇所のルートディレクトリを調べなければならず、たとえ何らかの方法で不正侵入できたととしても、複数箇

所のルートディレクトリの存在場所を知らない限り、全てのユーザーのパスワードを盗むことができなくなり、情報通信ネットワークシステムにおけるセキュリティを格段に向上させることができる。

【図面の簡単な説明】

【図 1】本発明にかかるパスワード認証システムの第 1 実施例を示すブロック図である。

【図 2】図 1 のパスワード認証システムによる処理手順を示すフローチャートである。

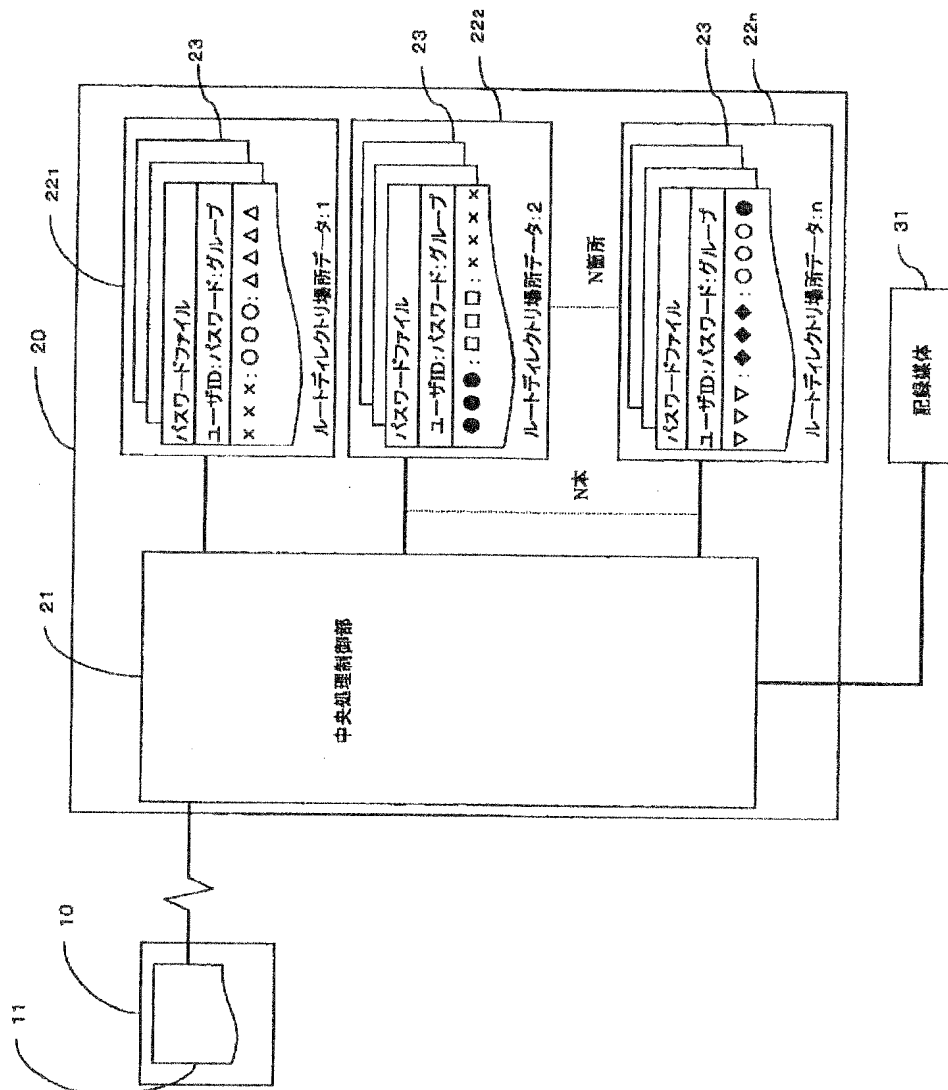
【図 3】本発明にかかるパスワード認証システムの第 2 実施例を示すブロック図である。

【符号の説明】

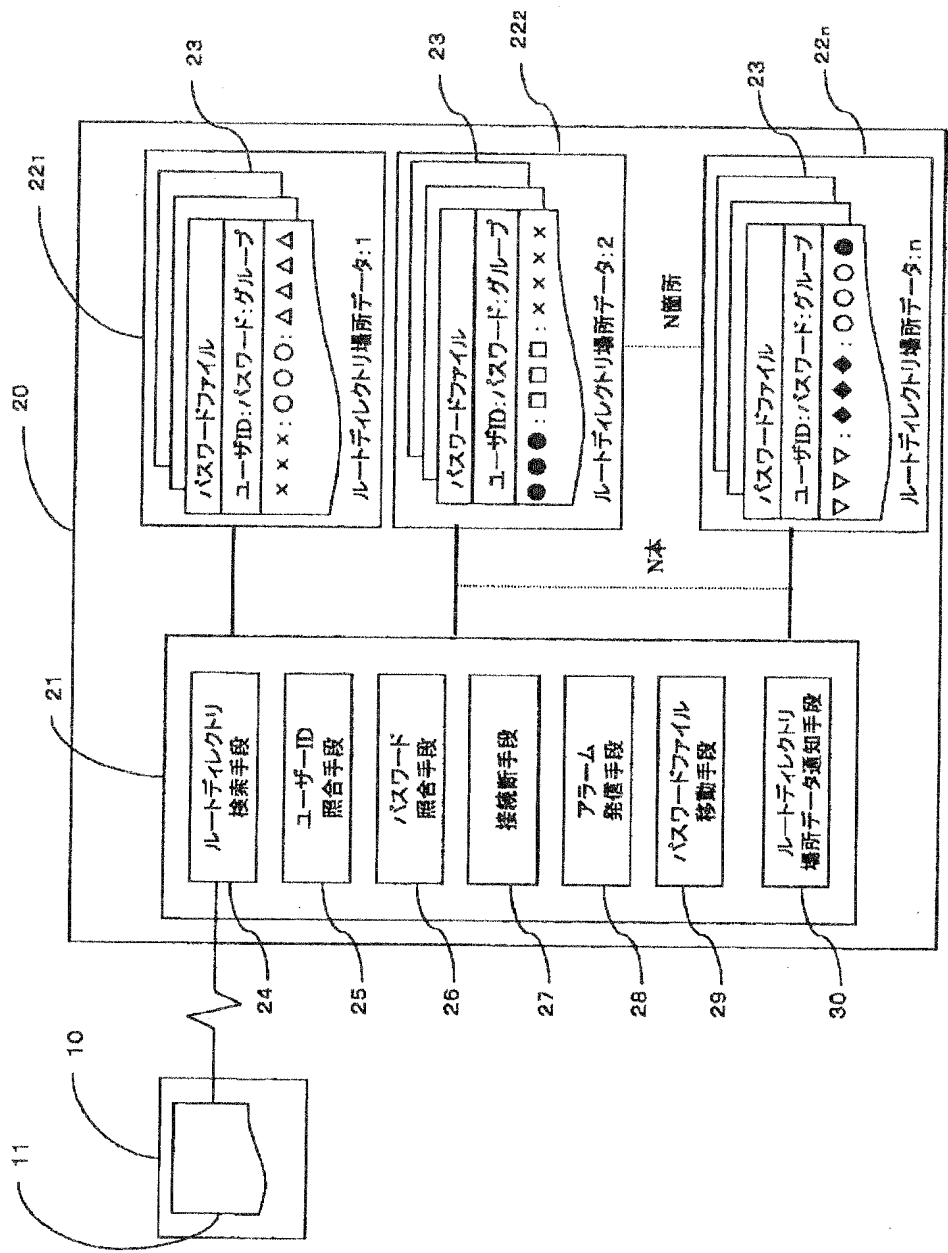
10 アクセス端末

- 11 記憶部
- 20 サーバー
- 21 中央処理制御部
- 22<sub>1</sub>～22<sub>n</sub> ルートディレクトリ
- 23 パスワードファイル
- 24 ルートディレクトリ検索手段
- 25 ユーザー ID 照合手段
- 26 パスワード照合手段
- 27 接続断手段
- 28 アラーム発信手段
- 29 パスワードファイル移動手段
- 30 ルートディレクトリ場所データ通知手段
- 31 記録媒体

【図 3】



【図 1】



【図2】

